

**LIGHTWEIGHT PUBLIC KEY INFRASTRUCTURE EMPLOYING  
UNSIGNED CERTIFICATES**

5

**Abstract of the Disclosure**

A public key infrastructure (PKI) includes a subject, a verifier, and certificate authority that issues a first unsigned certificate to the subject that binds a public key of the subject to long-term identification information related to the subject and maintains a certificate database of unsigned certificates in which it stores the first unsigned certificate. The verifier maintains a hash table containing cryptographic hashes of valid unsigned certificates corresponding to the unsigned certificates stored in the certificate database and including a cryptographic hash of the first unsigned certificate. The subject presents the issued first unsigned certificate to the verifier for authentication and demonstrates that the subject has knowledge of a private key corresponding to the public key in the unsigned certificate.

10

15

"Express Mail" mailing label number: EL3842491864S

Date of Deposit: 1-14-00

I hereby certify that this paper or fee is being deposited with the United States Postal Service "Express Mail Post Office to Addresses" service under 37 CFR 1.10 on the date indicated above and is addressed to the Assistant Commissioner for Patents,

Washington, D.C. 20231

Printed Name Christine Welter

Signature Christine Welter